The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/11/2012

SUBJECT:

Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (MS12-080)

OVERVIEW:

Two vulnerabilities have been reported in Microsoft Exchange Server that could allow for remote code execution or Denial of Service (DoS) conditions. Microsoft Exchange Server provides email, calendar and contacts for corporate environments.

Successful exploitation of one of the vulnerabilities could allow an attacker to run arbitrary code within the context of the LocalService account on the affected Microsoft Exchange Server. Typically, the LocalService account has minimum privileges on the system. Exploitation of the other vulnerability could cause Denial of Service (DoS) conditions.

SYSTEMS AFFECTED:

Microsoft Exchange Server 2007
Microsoft Exchange Server 2010

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: N/A

DESCRIPTION:

Two vulnerabilities have been discovered in Microsoft Exchange Server. The details of the vulnerabilities are as follows:

Oracle Outside In Contains Multiple Exploitable Vulnerabilities

This vulnerability occurs in the way the WebReady Document Viewing service parses files using the Oracle Outside In libraries. This issue exists due to vulnerabilities contained within libraries of Oracle Outside In. MS Exchange Server WebReady Document viewing is a feature that allows Outlook Web Access (OWA) users to view attachments such as Microsoft Office documents within the browser. **WebReady Document viewing is enabled by default.** This vulnerability can allow an attacker to run code on the Windows Exchange Server under the context of the LocalService account. If disabled, OWA users may not be able to preview the content of email attachments.

To exploit this vulnerability, an attacker creates a specially crafted file that is sent via e-mail to a user on a vulnerable version of Microsoft Exchange Server. When the user previews the document by clicking on the "Open as Webpage" link within OWA, the attacker's code runs within the privilege context of the LocalService account on the Microsoft Exchange Server. The LocalService account by default has limited system and file system privileges and sends only anonymous credentials over the network.

RSS Feed May Cause Exchange DoS Vulnerability

A DoS vulnerability exists due to the way MS Exchange handles Really Simple Syndication (RSS) Feeds. An attacker who successfully exploited this vulnerability could cause the Information Store service on the affected system to become unresponsive until the process is forcibly terminated. This unresponsive condition could cause Exchange databases to dismount, and potentially lead to corruption of databases, affecting user mailboxes.

In order for an attacker to exploit this vulnerability, they must have a valid email account on the Exchange server with the ability to create a specially crafted RSS feed, and then subscribe to that RSS feed. In turn, this creates a denial of service condition on the MS Exchange Server.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems after testing.
- Evaluate the relative need for WebReady Document viewing and disable if deemed non essential.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open un-trusted attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms12-080 http://support.microsoft.com/kb/2784126

SecurityFocus:

http://www.securityfocus.com/bid/55993
http://www.securityfocus.com/bid/55977
http://www.securityfocus.com/bid/56836

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3214
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3217
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4791